

ARTICLE APPEARED
ON PAGE 14-A

BALTIMORE SUN
11 June 1986

Recovery in Pelton case linked to Soviet countermeasures

By Charles W. Cordery
Washington Bureau of The Sun

WASHINGTON — The United States suffered still-uncalculated damage in the Pelton espionage case, and how long it takes to recover will depend on how clever the Russians are at using what they learned to foil U.S. high-technology spying devices, according to former intelligence officials.

George A. Carver Jr., a former CIA official and communications expert, said "there is nothing more vulnerable to compromises than intercepts" of another country's communications. Success depends heavily on the carelessness of the country being spied on and its having vulnerabilities that it does not know about, so that it does not know its codes and ciphers have been cracked and ought to be changed.

Mr. Carver judged the U.S. losses to be "incalculable," simply because the full range of injury is not yet known, but the effects almost certainly will be long lasting.

How long the recovery takes depends on how clever the Soviets are at using the data received from convicted spy Ronald W. Pelton to devise countermeasures against sophisticated U.S. eavesdropping devices, said retired Adm. Daniel Murphy, a former deputy director of central intelligence and a former intelligence overseer in the Defense Department.

U.S. intelligence-gathering has become such a delicate, complex, high-technology undertaking that it is increasingly vulnerable to having its secrets exposed.

This seems to be a lasting lesson of the Pelton spy case and, to some degree, of various other cases of Americans selling sensitive information to the Soviet Union over the past decade.

The simple reason for the vulnerability is that thousands, perhaps tens of thousands, of people at many levels of government and industry have to know something about the secret systems used to eavesdrop on the Soviets to collect military and political information.

"The field is rife with people who could be suborned," said retired Adm. Stansfield Turner, director of central intelligence in the Carter ad-

ministration. "We are in a new age of vulnerability to compromises of our technological intelligence systems."

When the systems are penetrated, it can take months or years to assess the damage and develop new devices that regain the lost capabilities. For all that was revealed about the Pelton case, the government is still unsure how much damage was done.

The House intelligence committee plans to pursue that point in closed hearings with officials of the National Security Agency, according to the committee's chief counsel, Michael J. O'Neil. The Senate intelligence committee is preparing an extensive report on the problems of counterintelligence — of catching spies.

In an interview, Mr. Turner saw the vulnerability of modern systems as the "significant point" brought home by the case of Pelton, convicted in Baltimore last week of selling secrets to the Soviets after a trial that gave unprecedented public exposure to the eavesdropping and code-breaking activities of the National Security Agency.

Pelton, employed as a communications specialist at the NSA for 14 years, declared bankruptcy and left the agency in 1979 and contacted the Soviet Embassy six months later, eventually receiving thousands of dollars for data on secret NSA projects. He was arrested last November, almost six years after his first contact with the Soviets.

"I fault the NSA for not realizing they had a highly volatile character on their hands," Mr. Turner said.

Another who stressed the vulnerability of U.S. high-tech intelligence-collection to espionage was Rudolph Hirsch, a former CIA employee and now acting director of computer and information systems at the University of Maryland.

A consultant on security and personnel practices, Mr. Hirsch said it should be standard practice for intelligence agencies to monitor their employees' solvency and, in cases of need, to aid them with loans, salary advances or loan guarantees.

In Mr. Hirsch's view, "anyone is a potential thief" if confronted by a severe enough financial emergency. He contended that an aid program such as the one he advocated could

have averted the current "spectacle" of trials involving allegations of secret-selling to the Soviet Union, China and Israel. Never in his own experience as a government consultant cleared for secret information, he added, had he been questioned about his finances, even when given polygraph tests.

U.S. intelligence-gathering today involves sophisticated submarine, surface and satellite eavesdropping devices, high-speed transmissions and supercomputers to sort out and help read coded communications.

The "bureaucratic process," with its constant rotation of government personnel, continually increases the numbers of people who know something about the complex systems, said Mr. Carver.

The Pelton case was replete with testimony that the Russians gained invaluable data on what the super-secret NSA knew about their communications links and thus how to take countermeasures to foil the U.S. eavesdroppers.

There was understandably a great deal less, if any, evidence indicating what Soviet countermeasures U.S. intelligence had detected and may already have learned how to circumvent.

Mr. Turner and Mr. Carver agreed that the damage may be longer lasting than that suffered from the Walker case, in which the Walker spy ring sold the Soviets information on hardware and software used by the Navy in coded communications.

The Navy said it had to step up production of new cryptographic equipment at a cost of "many millions of dollars" to restore its secure communications capability.

Through what they learned from Pelton — new information as well as information confirming what they already suspected — the Soviets have had to make their own moves to try to restore signals security and the NSA in turn has had to change its operations.

Mr. Turner said that "there will be a loss for a period of time" for America in the endless spy game of measures and countermeasures.

CONTINUED

2

Publicity given NSA operations in the Pelton case may have reinforced the Soviets' ideas about counter-measures they needed to take, Mr. Murphy said, but he doubted that "there was anything they didn't already suspect." As for America's damage assessment, "we know what we lost and we know what they should have learned." In such cases, the worst is usually assumed in patching up the damage.

All former intelligence officials consulted agreed that the government "wanted a conviction" in the Pelton case and thus was willing to reveal as much as it did about intelligence operations not previously discussed.

"They were sending a signal to others — this is what happens to you," said Mr. Hirsch. Mr. Murphy said the government "did a good job of walking a fine line" in revealing enough for a conviction. Mr. Turner was "surprised that they spoke openly of decoding anybody's messages," but "they wanted a conviction" and made the necessary trade-offs.

Admiral Murphy was U.S. 6th Fleet commander in the Mediterranean at the time of the 1973 Arab-Israeli war and now realizes that all his plans for dealing with the Soviet fleet, if it came to that, could have been compromised by the Walker ring. "I'll never know," he said.